What is claimed is

1. An elliptic curve exponentiation apparatus that computes an elliptic curve exponentiation for an elliptic curve $E: y^2=x^3+a\times x+b$ defined over a residue field F with a prime p being a modulus, comprising:

an information obtaining unit operable to obtain a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

a first storage unit operable to store therein a coefficient a that is an x term of the elliptic curve E;

a computation unit operable to compute an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point $k*Q$;

a judgment unit operable to judge whether the obtained exponentiation-result-point $k*Q$ is on the elliptic curve E; and

an output unit operable to output the obtained exponentiation-result-point $k*Q$, when a judgment result of the judging unit is affirmative.

2. The elliptic curve exponentiation apparatus of Claim 1, further comprising

a second storage unit operable to store therein a

coefficient b that is a constant term of the elliptic curve E,

wherein the judgment unit judges whether the obtained exponentiation-result-point $k*Q$ is on the elliptic curve E, using the coefficient a stored in the first storage unit and the coefficient b stored in the second storage unit.

3. The elliptic curve exponentiation apparatus of Claim 2, further comprising

a constant term coefficient obtaining unit operable to obtain the coefficient b, and write the obtained coefficient b into the second storage unit.

4. The elliptic curve exponentiation apparatus of Claim 2, further comprising

an x term coefficient obtaining unit operable to obtain the coefficient a, and write the obtained coefficient a into the first storage unit.

5. The elliptic curve exponentiation apparatus of Claim 2, further comprising

a constant term coefficient computation unit operable to compute the coefficient b, using the coefficient a stored in the first storage unit, the obtained point Q, and the elliptic curve $E: y^2=x^3+a\times x+b$, and write the computed coefficient b into

the second storage unit.

6. The elliptic curve exponentiation apparatus of Claim 5, wherein

the computation unit computes coordinates (Qx, Qy) as the exponentiation-result-point $k*Q$, and

the judgment unit computes $(Qy)^2$ and $(Qx)^3+a\times Qx+b$, compares a computation result of $(Qy)^2$ and a computation result of $(Qx)^3+a\times Qx+b$, and when the computation result of $(Qy)^2$ and the computation result of $(Qx)^3+a\times Qx+b$ match, judges that the exponentiation-result-point $k*Q$ is on the elliptic curve E.

7. The elliptic curve exponentiation apparatus of Claim 5, further comprising

an error message output unit operable to output a message indicating that an error has occurred, when the judgment unit judges that the exponentiation-result-point $k*Q$ is not on the elliptic curve E.

8. The elliptic curve exponentiation apparatus of Claim 1, wherein

the judgment unit judges whether the point Q and the exponentiation-result-point $k*Q$ are on a same elliptic curve,

instead of judging whether the exponentiation-result-point $k*Q$ is on the elliptic curve E, and

the output unit outputs the exponentiation-result-point $k*Q$ when the judgment unit judges that the point Q and the exponentiation-result-point $k*Q$ are on the same elliptic curve, instead of when the judgment unit judges that the exponentiation-result-point $k*Q$ is on the elliptic curve E.

9. The elliptic curve exponentiation apparatus of Claim 8, wherein

the information obtaining unit obtains coordinates (Qx, Qy) as the point Q,

the computation unit computes coordinates (Qx', Qy') as the exponentiation-result-point $k*Q$, and

the judgment unit judges whether the point Q and the exponentiation-result-point $k*Q$ are on the same elliptic curve, by judging whether $(Qy^2-Qx^3-a\times Qx)-(Qy'^2-Qx'^3-a\times Qx')=0$.

10. An information security apparatus that ensures secure handling of predetermined information by computing an elliptic curve exponentiation of $k*Q$, based on computational complexity of solving a discrete logarithm problem on an elliptic curve $E: y^2=x^3+a\times x+b$ defined over a residue field F with a prime p being a modulus, comprising:

an information obtaining unit operable to obtain a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

a first storage unit operable to store therein a coefficient a that is an x term of the elliptic curve E;

a computation unit operable to compute an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point $k*Q$;

a judgment unit operable to judge whether the obtained exponentiation-result-point $k*Q$ is on the elliptic curve E; and

a prohibition unit operable to prohibit an output of the obtained exponentiation-result-point $k*Q$, when a judgment result of the judging unit is negative.

11. The information security apparatus of Claim 10, wherein

the elliptic curve exponentiation of $k*Q$ is computed, to realize processes of: encryption of a plaintext, decryption of a ciphertext; generation of a signature for a plaintext; signature verification for a plaintext and a signature; or a process of sharing of a secret key between two parties without revealing the secret key to a third party.

12. An elliptic curve exponentiation method for use in an elliptic curve exponentiation apparatus that computes an elliptic curve exponentiation for an elliptic curve $E: y^2=x^3+a \times x+b$ defined over a residue field F with a prime p being a modulus, and that includes an information obtaining unit, a first storage unit storing a coefficient a that is an x term of the elliptic curve E, a computation unit, a judgment unit, and an output unit, the method comprising:

an information obtaining step, executed by the information obtaining unit, of obtaining a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

a computation step, executed by the computation unit, of computing an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point $k*Q$;

a judgment step, executed by the judgment unit, of judging whether the obtained exponentiation-result-point $k*Q$ is on the elliptic curve E; and

an output step, executed by the output unit, of outputting the obtained exponentiation-result-point $k*Q$, when a judgment result in the judging step is affirmative.

13. A computer program for computation of an elliptic curve exponentiation, for use in an elliptic curve

exponentiation apparatus that computes an elliptic curve exponentiation for an elliptic curve $E: y^2=x^3+a\times x+b$ defined over a residue field F with a prime p being a modulus, and that includes an information obtaining unit, a first storage unit storing a coefficient a that is an x term of the elliptic curve E, a computation unit, a judgment unit, and an output unit, the program comprising:

an information obtaining step, executed by the information obtaining unit, of obtaining a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

a computation step, executed by the computation unit, of computing an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point $k*Q$;

a judgment step, executed by the judgment unit, of judging whether the obtained exponentiation-result-point $k*Q$ is on the elliptic curve E; and

an output step, executed by the output unit, of outputting the obtained exponentiation-result-point $k*Q$, when a judgment result in the judging step is affirmative.

14. The computer program of Claim 13, recorded on a computer-readable recording medium.